

CLAIMS

1. A method of preventing theft of decompressed digital content as the content is being rendered, the method comprising:

detecting a requested slow-down of the rendering of the content, wherein the detected requested slow-down is presumably initiated by a content thief attempting to steal the content; and

responding to the detected requested slow-down in a manner designed to frustrate the presumed attempt of the content thief to steal the content.

2. The method of claim 1 wherein responding comprises ignoring requests for the slow-down.

3. The method of claim 1 wherein responding comprises ignoring requests for the slow-down after receiving a pre-determined number of such requests.

4. The method of claim 1 wherein responding comprises stopping rendering of the content.

5. The method of claim 1 wherein responding comprises slowing rendering of the content to a rate smaller than that of the requested slow-down.

6. The method of claim 1 wherein responding comprises degrading rendering of the content.

TO 290" 2323350

7. The method of claim 1 wherein rendering of the content occurs on a processor having an amount of capacity, and wherein responding comprises reserving a relatively large amount of the capacity of the processor for rendering, the reserved capacity not being available to the content thief for use in stealing the content.

8. The method of claim 1 wherein detecting the slow-down comprises noting a reduction in a rate of rendering of the content.

9. The method of claim 1 wherein detecting the slow-down comprises noting requests for individual renderings of frames of the content.

10. A method of preventing theft of decompressed digital content as the content is being rendered, the method comprising:

detecting transfers of relatively large amounts of data, wherein the detected transfers are presumably initiated by a content thief attempting to steal the content; and

responding to the detected transfers in a manner designed to frustrate the presumed attempt of the content thief to steal the content.

11. The method of claim 10 wherein responding comprises stopping rendering of the content.

12. The method of claim 10 wherein responding comprises slowing rendering of the content.

13. The method of claim 10 wherein responding comprises degrading rendering of the content.

14. The method of claim 10 wherein rendering of the content occurs on a processor having an amount of capacity, and wherein responding

0499223.062701
T07290" 03225850

comprises reserving a relatively large amount of the capacity of the processor for rendering, the reserved capacity not being available to the content thief for use in stealing the content.

15. A method of preventing theft of decompressed digital content as the content is being rendered, the method comprising:

detecting a re-compressor-based requested slow-down of the rendering of the content, wherein the detected requested slow-down is presumably initiated by a content thief attempting to steal and re-compress the content; and

responding to the detected requested slow-down in a manner designed to frustrate the presumed attempt of the content thief to steal and re-compress the content.

16. The method of claim 15 wherein detecting comprises sensing X consecutive SEEK or STEP operations.

17. The method of claim 16 wherein detecting comprises sensing 30 consecutive SEEK or STEP operations.

18. The method of claim 15 wherein detecting comprises consulting all available clocks and determining therefrom if rendering is occurring at less than real-time speed.

19. The method of claim 15 wherein detecting comprises sensing excessive SEEK and GET_POS commands.

20. The method of claim 15 wherein responding comprises ignoring control operations such as SEEK and STEP for Y seconds.

10/22/2004 10:22:50

21. The method of claim 20 wherein responding comprises ignoring control operations such as SEEK and STEP for 30 seconds.
22. The method of claim 15 wherein responding comprises performing a non-responsive action.
23. The method of claim 22 wherein responding comprises performing a non-responsive action selected from a group consisting of rendering at real-time speed, intentionally omitting rendering of frames, and stopping rendering.
24. The method of claim 15 wherein responding comprises providing requested data with a built-in error.
25. The method of claim 24 wherein responding comprises providing requested data with a built-in error which gets progressively worse.
26. A method of preventing theft of decompressed digital content as the content is being rendered, the method comprising:
detecting a re-compressor re-compressing the content, wherein the detected re-compressor is presumably operated by a content thief attempting to steal and re-compress the content; and
responding to the detected re-compressor in a manner designed to frustrate the presumed attempt of the content thief to steal and re-compress the content.
27. The method of claim 26 wherein rendering of the content occurs on a processor having an amount of capacity, and wherein detecting comprises sensing a process employing at least a pre-determined amount of the capacity of the processor.

28. The method of claim 26 wherein responding comprises stopping rendering of the content.

29. The method of claim 26 wherein rendering of the content occurs on a processor having an amount of capacity, and wherein responding comprises controlling the capacity of the processor available for other processes.

30. A computer-readable medium having computer-executable instructions thereon for preventing theft of decompressed digital content as the content is being rendered, the instructions being organized into modules including:

a first module for detecting a requested slow-down of the rendering of the content, wherein the detected requested slow-down is presumably initiated by a content thief attempting to steal the content; and

a second module for responding to the detected requested slow-down in a manner designed to frustrate the presumed attempt of the content thief to steal the content.

31. The medium of claim 30 wherein the second module ignores requests for the slow-down.

32. The medium of claim 30 wherein the second module ignores requests for the slow-down after receiving a pre-determined number of such requests.

33. The medium of claim 30 wherein the second module stops rendering of the content.

34. The medium of claim 30 wherein the second module slows rendering of the content to a rate smaller than that of the requested slow-down.

FOIA b 7 - DATED 08/22/2013



35. The medium of claim 30 wherein the second module degrades rendering of the content.

36. The medium of claim 30 wherein rendering of the content occurs on a processor having an amount of capacity, and wherein the second module reserves a relatively large amount of the capacity of the processor for rendering, the reserved capacity not being available to the content thief for use in stealing the content.

37. The medium of claim 30 wherein the first module notes a reduction in a rate of rendering of the content.

38. The medium of claim 30 wherein the first module notes requests for individual renderings of frames of the content.

39. A computer-readable medium having computer-executable instructions thereon for preventing theft of decompressed digital content as the content is being rendered, the instructions being organized into modules including:

a first module for detecting transfers of relatively large amounts of data, wherein the detected transfers are presumably initiated by a content thief attempting to steal the content; and

a second module for responding to the detected transfers in a manner designed to frustrate the presumed attempt of the content thief to steal the content.

40. The medium of claim 39 wherein the second module stops rendering of the content.

41. The medium of claim 39 wherein the second module slows rendering of the content.

42. The medium of claim 39 wherein the second module degrades rendering of the content.

43. The medium of claim 39 wherein rendering of the content occurs on a processor having an amount of capacity, and wherein the second module reserves a relatively large amount of the capacity of the processor for rendering, the reserved capacity not being available to the content thief for use in stealing the content.

44. A computer-readable medium having computer-executable instructions thereon for preventing theft of decompressed digital content as the content is being rendered, the instructions being organized into modules including:

a first module for detecting a re-compressor-based requested slow-down of the rendering of the content, wherein the detected requested slow-down is presumably initiated by a content thief attempting to steal and re-compress the content; and

a second module for responding to the detected requested slow-down in a manner designed to frustrate the presumed attempt of the content thief to steal and re-compress the content.

45. The medium of claim 44 wherein the first module senses X consecutive SEEK or STEP operations.

46. The medium of claim 45 wherein the first module senses 30 consecutive SEEK or STEP operations.

47. The medium of claim 44 wherein the first module consults all available clocks and determining therefrom if rendering is occurring at less than real-time speed.

10/29/2007 10:26:50

48. The medium of claim 44 wherein the first module senses excessive SEEK and GET_POS commands.

49. The medium of claim 44 wherein the second module ignores control operations such as SEEK and STEP for Y seconds.

50. The medium of claim 49 wherein the second module ignores control operations such as SEEK and STEP for 30 seconds.

51. The medium of claim 44 wherein the second module performs a non-responsive action.

52. The medium of claim 51 wherein the second module performs a non-responsive action selected from a group consisting of rendering at real-time speed, intentionally omitting rendering of frames, and stopping rendering.

53. The medium of claim 44 wherein the second module provides requested data with a built-in error.

54. The medium of claim 53 wherein the second module provides requested data with a built-in error which gets progressively worse.

55. A computer-readable medium having computer-executable instructions thereon for preventing theft of decompressed digital content as the content is being rendered, the instructions being organized into modules including:

a first module for detecting a re-compressor re-compressing the content, wherein the detected re-compressor is presumably operated by a content thief attempting to steal and re-compress the content; and

a second module for responding to the detected re-compressor in a manner designed to frustrate the presumed attempt of the content thief to steal and re-compress the content.

10/22/99 4:03:26 PM

56. The medium of claim 53 wherein rendering of the content occurs on a processor having an amount of capacity, and wherein the first module senses a process employing at least a pre-determined amount of the capacity of the processor.

57. The medium of claim 53 wherein the second module stops rendering of the content.

58. The medium of claim 53 wherein rendering of the content occurs on a processor having an amount of capacity, and wherein the second module controls the capacity of the processor available for other processes.

10/22/2010 10:22:26 AM